NP-Intermediate Problems and Quantum Algorithms

Tristram Bogart

Universidad de los Andes

31 May 2013
Outline

- Complexity classes and graph theory
- The graph isomorphism problem
- The hidden subgroup problem and quantum algorithms
- The abelian case
- The symmetric group case and graph isomorphisms
A (yes-no) decision problem is in complexity class $P$ if there is a algorithm (Turing machine) to solve it and a polynomial $p$ such that for all $n$ and all input of bit-length $n$, the algorithm terminates correctly in at most $p(n)$ steps.
P and NP

A (yes-no) decision problem is in complexity class $P$ if there is a algorithm (Turing machine) to solve it and a polynomial $p$ such that for all $n$ and all input of bit-length $n$, the algorithm terminates correctly in at most $p(n)$ steps.

A decision problem is in class $NP$ if a 'yes' answer can always be verified in polynomial time with the aid of an appropriate certificate. A problem is in co-$NP$ if a 'no' answer can be similarly verified.
P and NP

A (yes-no) decision problem is in complexity class $P$ if there is an algorithm (Turing machine) to solve it and a polynomial $p$ such that for all $n$ and all input of bit-length $n$, the algorithm terminates correctly in at most $p(n)$ steps.

A decision problem is in class $NP$ if a ’yes’ answer can always be verified in polynomial time with the aid of an appropriate certificate. A problem is in co-$NP$ if a ’no’ answer can be similarly verified.

Note that $P \subseteq NP \cap co-NP$.

Million-dollar question: Does $P$ equal $NP$?
Graph problems in \( P \)

A graph is a finite set \( V \) of vertices and a set \( E \) of edges, given as pairs of vertices.

The following graph theoretic problems are in \( P \):

- **Connected**: Given a graph \( \Gamma \), is there a path between every pair of vertices?
- **Bipartite**: Given a graph \( \Gamma \), can its vertices be partitioned into two sets \( A \) and \( B \) such that every edge has one end in \( A \) and the other in \( B \)?
- **Eulerian circuit**: Given a graph \( \Gamma \), does \( \Gamma \) contain a (closed) circuit that includes each edge of \( \Gamma \) exactly once?
Graph problems in $P$

A graph is a finite set $V$ of vertices and a set $E$ of edges, given as pairs of vertices.

The following graph theoretic problems are in $P$:

- **Connected**: Given a graph $\Gamma$, is there a path between every pair of vertices?
- **Bipartite**: Given a graph $\Gamma$, can its vertices be partitioned into two sets $A$ and $B$ such that every edge has one end in $A$ and the other in $B$?
- **Eulerian circuit**: Given a graph $\Gamma$, does $\Gamma$ contain a (closed) circuit that includes each edge of $\Gamma$ exactly once?

A graph has an Eulerian circuit if and only if every vertex has even degree.
Graph problems in NP

- **k-Clique**: Given a graph $\Gamma$ and a number $k$, does $\Gamma$ contain a complete subgraph with $k$ vertices?
- **k-Chromatic**: Given a graph $\Gamma$ and a number $k$, can the vertices of $\Gamma$ be colored with $k$ colors such that no two adjacent vertices have the same color?
- **Hamiltonian**: Given a graph $\Gamma$, does $\Gamma$ contain a cycle that passes through each vertex exactly once?
- **Graph Isomorphism**: Given graphs $\Gamma_1$ and $\Gamma_2$, is there a bijection $f$ from the vertices of $\Gamma_1$ to the vertices of $\Gamma_2$ such that $\{u, v\}$ is an edge of $\Gamma_1$ if and only if $\{f(u), f(v)\}$ is an edge of $\Gamma_2$?
Graph problems in NP

- **k-Clique**: Given a graph $\Gamma$ and a number $k$, does $\Gamma$ contain a complete subgraph with $k$ vertices?

- **k-Chromatic**: Given a graph $\Gamma$ and a number $k$, can the vertices of $\Gamma$ be colored with $k$ colors such that no two adjacent vertices have the same color?

- **Hamiltonian**: Given a graph $\Gamma$, does $\Gamma$ contain a cycle that passes through each vertex exactly once?

- **Graph Isomorphism**: Given graphs $\Gamma_1$ and $\Gamma_2$, is there a bijection $f$ from the vertices of $\Gamma_1$ to the vertices of $\Gamma_2$ such that $\{u, v\}$ is an edge of $\Gamma_1$ if and only if $\{f(u), f(v)\}$ is an edge of $\Gamma_2$?

In each case, the desired object is itself a certificate whenever the answer is YES. None of the problems are known to be in co-NP.
A problem $X$ is

- **NP-hard** if every problem in $NP$ can be reduced to $X$ in polynomial time.
- **NP-complete** if it is both in $NP$ and NP-hard.
- **NP-intermediate** if it is NP, but neither in P nor NP-Hard.

By definition, if some NP-complete problem can be solved in polynomial-time, then $P=NP$. 
A problem $X$ is

- **NP-hard** if every problem in $NP$ can be reduced to $X$ in polynomial time.
- **NP-complete** if it is both in $NP$ and NP-hard.
- **NP-intermediate** if it is NP, but neither in P nor NP-Hard.

By definition, if some NP-complete problem can be solved in polynomial-time, then $P=NP$.

**Theorem (Cook, '71)** The problem SAT (satisfiability of Boolean functions) is NP-complete.

**Theorem (Karp, '72)** The problems $k$-Clique, $k$-Chromatic, Hamiltonian (and several others) are NP-complete.
**NP-completeness**

A problem $X$ is

- **NP-hard** if every problem in $NP$ can be reduced to $X$ in polynomial time.
- **NP-complete** if it is both in $NP$ and NP-hard.
- **NP-intermediate** if it is $NP$, but neither in $P$ nor NP-Hard.

By definition, if some NP-complete problem can be solved in polynomial-time, then $P=NP$.

**Theorem (Cook, ’71)** The problem SAT (satisfiability of Boolean functions) is NP-complete.

**Theorem (Karp, ’72)** The problems $k$-Clique, $k$-Chromatic, Hamiltonian (and several others) are NP-complete.

In fact most problems in $NP$ are either known to be in $P$ or are NP-complete. Graph Isomorphism is an exception, as is factoring.
Friendliness of Graph Isomorphism

- There are polynomial-time algorithms for important special cases such as planar graphs, graphs of bounded vertex degree, and graphs whose adjacency matrices have bounded eigenvalue multiplicity.
- Non-isomorphic graphs usually can be easily distinguished by degree sequence, counting small subgraphs, or eigenvalues of the adjacency matrix.
- There are algorithms that usually run in polynomial time in practice, though take exponential time in the worst case.
- The problem of counting isomorphisms reduces in polynomial time to the decision problem, unlike for many NP-hard problems.
Isomorphisms and automorphisms

Let $\Gamma_1$ and $\Gamma_2$ be graphs on $n$ vertices and $\Gamma$ be their disjoint union. An isomorphism between $\Gamma_1$ and $\Gamma_2$ is an automorphism $\sigma$ of $\Gamma$ that interchanges $V(\Gamma_1)$ with $V(\Gamma_2)$. 
Isomorphisms and automorphisms

Let $\Gamma_1$ and $\Gamma_2$ be graphs on $n$ vertices and $\Gamma$ be their disjoint union. An isomorphism between $\Gamma_1$ and $\Gamma_2$ is an automorphism $\sigma$ of $\Gamma$ that interchanges $V(\Gamma_1)$ with $V(\Gamma_2)$.

Given generators of $\text{Aut}(\Gamma)$, we can check in polynomial time if any automorphism has the interchange property. So Graph Isomorphism reduces to finding generators for $\text{Aut}(\Gamma) \leq S_{2n}$, a special case of ...
The hidden subgroup problem

Given a finite group $G$, find generators of an unknown subgroup $H$. We are allowed to call a function $f$ on $G$ that satisfies:

$$f(x) = f(y) \iff x, y \text{ are in the same coset of } H.$$
The hidden subgroup problem

Given a finite group $G$, find generators of an unknown subgroup $H$. We are allowed to call a function $f$ on $G$ that satisfies:

$$f(x) = f(y) \iff x, y \text{ are in the same coset of } H.$$  

**Example:** Let $G = \mathbb{Z}^3_2 = \langle y_1, y_2, y_3 \rangle$ and $H = \langle y_1 + y_2 \rangle$, a two-element subgroup. Define $f : G \to \mathbb{Z}_2^2$ by $f(a, b, c) = (a + b, c)$. Then $f$ is constant on the cosets of $H$ and distinguishes them.
The hidden subgroup problem

Given a finite group $G$, find generators of an unknown subgroup $H$. We are allowed to call a function $f$ on $G$ that satisfies:

$$f(x) = f(y) \iff x, y \text{ are in the same coset of } H.$$ 

**Example:** Let $G = \mathbb{Z}_2^3 = \langle y_1, y_2, y_3 \rangle$ and $H = \langle y_1 + y_2 \rangle$, a two-element subgroup. Define $f : G \to \mathbb{Z}_2^2$ by $f(a, b, c) = (a + b, c)$. Then $f$ is constant on the cosets of $H$ and distinguishes them.

To solve the hidden subgroup problem, we will study representations of the group $G$: homomorphisms $\rho$ from $G$ to $\text{GL}_n(\mathbb{C})$. The number $d_\rho := n$ is the dimension of the representation. The character $\chi_\rho(g)$ is the trace of the matrix $\rho(g)$. 
A quantum algorithm for the HSP

Define a state $|g\rangle$ for each $g \in G$. Define states $|(\rho, i, j)\rangle$ for each irreducible representation $\rho$ and each matrix entry $(i, j)$.
A quantum algorithm for the HSP

Define a state $|g\rangle$ for each $g \in G$. Define states $|(\rho, i, j)\rangle$ for each irreducible representation $\rho$ and each matrix entry $(i, j)$.

Define the following operators:

- An operator $S$ that superposes the elements of $G$.
- An operator $U_f$ that evaluates $f$; that is,

$$U_f (|g\rangle \otimes |00\ldots0\rangle) = |g\rangle \otimes |f(g)\rangle$$

- The quantum Fourier transform $\mathcal{F}$ that superposes all possible irreducible representations of a given element of $G$.

For appropriate groups $G$, each can be implemented with polynomially many basic quantum operations.
A quantum algorithm for the HSP, continued

- Initialize two quantum registers, one for elements of $G$ and another for values of $f$.

- Apply $S$ to the first register to get

$$\frac{1}{\sqrt{|G|}} \sum_{g \in G} |g\rangle \otimes |00 \ldots 0\rangle .$$

- Apply $U_f$ to get

$$\frac{1}{\sqrt{|G|}} \sum_{g \in G} |g\rangle \otimes |f(g)\rangle .$$

- Measure the second register. The result is $f(c)$ for some random $c \in G$, giving

$$\frac{1}{\sqrt{|H|}} \sum_{h \in H} |hc\rangle \otimes |f(c)\rangle .$$
Ignore the second register and apply $\mathcal{F}$ to the first, giving

$$
\sum_{\rho \text{ irrep of } G} \frac{d_{\rho}}{\sqrt{|G||H|}} \left( \sum_{h \in H} \rho(ch)_{i,j} |\rho, i, j\rangle \right).
$$

Measure the representation $\rho$. The probability of a given $\rho$ is

$$
d_{\rho} \frac{\sum_{h \in H} \chi_{\rho}(h)}{|G|}.
$$

Repeat enough times to effectively sample $H$. 

A quantum algorithm for the HSP, continued
Representations of abelian groups

The representations of a cyclic group $\mathbb{Z}_n = \langle y \rangle$ are all one-dimensional, given by $y \mapsto e^{\frac{2\pi i k}{n}}, \ 0 \leq k \leq n - 1$. The quantum Fourier transform in this case is the regular Fourier transform.

In particular, for $\mathbb{Z}_2$, we have the trivial representation given by $y \mapsto 1$ and the sign representation given by $y \mapsto -1$. 
Representations of abelian groups

The representations of a cyclic group \( \mathbb{Z}_n = \langle y \rangle \) are all one-dimensional, given by \( y \mapsto e^{\frac{2\pi i k}{n}}, \ 0 \leq k \leq n - 1 \). The quantum Fourier transform in this case is the regular Fourier transform.

In particular, for \( \mathbb{Z}_2 \), we have the trivial representation given by \( y \mapsto 1 \) and the sign representation given by \( y \mapsto -1 \).

For \( \mathbb{Z}_2^n = \langle y_1, y_2, \ldots, y_n \rangle \) we have \( 2^n \) representations given by \( y_i \mapsto \pm 1 \) for each \( i \). Given such a \( \rho \),

\[
\rho \left( \sum_{i \in I} y_i \right) = -1 \# \{ i \in I : \rho(y_i) = -1 \}.
\]

That is, the representations give the (vector space) dual to \( \mathbb{Z}_2^n \).
An abelian example

Let $G = \mathbb{Z}_2^3 = \langle y_1, y_2, y_3 \rangle$ and $H = \langle y_1 + y_2 \rangle \cong \mathbb{Z}_2$.

<table>
<thead>
<tr>
<th>$\rho$</th>
<th>$\rho(e)$</th>
<th>$\rho(y_1 + y_2)$</th>
<th>Prob($\rho$)</th>
</tr>
</thead>
<tbody>
<tr>
<td>(+,+,+)</td>
<td>1</td>
<td>1</td>
<td>2/8</td>
</tr>
<tr>
<td>(+,+-)</td>
<td>1</td>
<td>1</td>
<td>2/8</td>
</tr>
<tr>
<td>(+,-,+)</td>
<td>1</td>
<td>-1</td>
<td>0</td>
</tr>
<tr>
<td>(+,-,-)</td>
<td>1</td>
<td>-1</td>
<td>0</td>
</tr>
<tr>
<td>(-,+,+)</td>
<td>1</td>
<td>-1</td>
<td>0</td>
</tr>
<tr>
<td>(-,+-)</td>
<td>1</td>
<td>-1</td>
<td>0</td>
</tr>
<tr>
<td>(-,-,+)</td>
<td>1</td>
<td>1</td>
<td>2/8</td>
</tr>
<tr>
<td>(-,-,-)</td>
<td>1</td>
<td>1</td>
<td>2/8</td>
</tr>
</tbody>
</table>
An abelian example

Let $G = \mathbb{Z}_2^3 = \langle y_1, y_2, y_3 \rangle$ and $H = \langle y_1 + y_2 \rangle \cong \mathbb{Z}_2$.

<table>
<thead>
<tr>
<th>$\rho$</th>
<th>$\rho(e)$</th>
<th>$\rho(y_1 + y_2)$</th>
<th>Prob($\rho$)</th>
</tr>
</thead>
<tbody>
<tr>
<td>(+,+,+)</td>
<td>1</td>
<td>1</td>
<td>2/8</td>
</tr>
<tr>
<td>(+,+,−)</td>
<td>1</td>
<td>1</td>
<td>2/8</td>
</tr>
<tr>
<td>(+,−,+)</td>
<td>1</td>
<td>−1</td>
<td>0</td>
</tr>
<tr>
<td>(+,−,−)</td>
<td>1</td>
<td>−1</td>
<td>0</td>
</tr>
<tr>
<td>(−,+,+)</td>
<td>1</td>
<td>−1</td>
<td>0</td>
</tr>
<tr>
<td>(−,+,−)</td>
<td>1</td>
<td>−1</td>
<td>0</td>
</tr>
<tr>
<td>(−,−,+)</td>
<td>1</td>
<td>1</td>
<td>2/8</td>
</tr>
<tr>
<td>(−,−,−)</td>
<td>1</td>
<td>1</td>
<td>2/8</td>
</tr>
</tbody>
</table>

Thus the algorithm gives a random representation dual to $H$. The same holds for any subgroup $K$ of $\mathbb{Z}_2^n$. With high probability, $K^*$ is generated by $2n$ random elements of it. Finally, $K^*$ determines $K$. 
Irreducible representations of the symmetric group $S_3$

- Trivial representation: $\rho_{\text{triv}}(\sigma) = 1$ for all permutations $\sigma$.

- Sign representation: $\rho_{\text{sign}}(\sigma) = \begin{cases} 1 & \text{if } \sigma \text{ is even} \\ -1 & \text{if } \sigma \text{ is odd} \end{cases}$

- Standard representation $\rho_{\text{std}}$: let $S_3$ act on $\mathbb{C}^3$ by permuting coordinates. Restrict the action to the plane given by $x_1 + x_2 + x_3 = 0$. Choose a basis for the plane: say $\{e_1 - e_2, e_2 - e_3\}$. 
Irreducible representations of the symmetric group $S_3$

- Trivial representation: $\rho_{\text{triv}}(\sigma) = 1$ for all permutations $\sigma$.

- Sign representation: $\rho_{\text{sign}}(\sigma) = \begin{cases} 1 & \text{if } \sigma \text{ is even} \\ -1 & \text{if } \sigma \text{ is odd} \end{cases}$

- Standard representation $\rho_{\text{std}}$: let $S_3$ act on $\mathbb{C}^3$ by permuting coordinates. Restrict the action to the plane given by $x_1 + x_2 + x_3 = 0$. Choose a basis for the plane: say $\{e_1 - e_2, e_2 - e_3\}$.

The respective dimensions are 1, 1, and 2. Since $1^2 + 1^2 + 2^2 = 6 = |S_3|$, Matschke’s theorem guarantees that they are the only irreducible representations of $S_3$ over $\mathbb{C}$.
### Sampling subgroups of $S_3$

<table>
<thead>
<tr>
<th>$\sigma \in S_3$</th>
<th>$\rho_{\text{triv}}(\sigma)$</th>
<th>$\rho_{\text{sgn}}(\sigma)$</th>
<th>$\rho_{\text{std}}(\sigma)$</th>
<th>$\chi_{\text{std}}(\sigma)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$e$</td>
<td>1</td>
<td>1</td>
<td>$\begin{pmatrix} 1 &amp; 0 \ 0 &amp; 1 \end{pmatrix}$</td>
<td>2</td>
</tr>
<tr>
<td>(12)</td>
<td>1</td>
<td>-1</td>
<td>$\begin{pmatrix} -1 &amp; 1 \ 0 &amp; 1 \end{pmatrix}$</td>
<td>0</td>
</tr>
<tr>
<td>(23)</td>
<td>1</td>
<td>-1</td>
<td>$\begin{pmatrix} 1 &amp; 0 \ 1 &amp; -1 \end{pmatrix}$</td>
<td>0</td>
</tr>
<tr>
<td>(13)</td>
<td>1</td>
<td>-1</td>
<td>$\begin{pmatrix} 0 &amp; -1 \ -1 &amp; 0 \end{pmatrix}$</td>
<td>0</td>
</tr>
<tr>
<td>(123)</td>
<td>1</td>
<td>1</td>
<td>$\begin{pmatrix} 0 &amp; -1 \ 1 &amp; -1 \end{pmatrix}$</td>
<td>-1</td>
</tr>
<tr>
<td>(132)</td>
<td>1</td>
<td>1</td>
<td>$\begin{pmatrix} -1 &amp; 1 \ -1 &amp; 0 \end{pmatrix}$</td>
<td>2</td>
</tr>
</tbody>
</table>
Sampling subgroups of $S_3$, continued

For the trivial group $\{e\}$:

\[
\begin{align*}
\Pr(\rho_{\text{triv}}) &= 1 \cdot \frac{\chi_{\text{triv}}(e)}{6} = \frac{1}{6} \\
\Pr(\rho_{\text{sgn}}) &= 1 \cdot \frac{\chi_{\text{sgn}}(e)}{6} = \frac{1}{6} \\
\Pr(\rho_{\text{std}}) &= 2 \cdot \frac{\chi_{\text{std}}(e)}{6} = \frac{4}{6}
\end{align*}
\]
Sampling subgroups of $S_3$, continued

For the trivial group $\{e\}$:

\[
\begin{align*}
\Pr(\rho_{\text{triv}}) &= 1 \cdot \frac{\chi_{\text{triv}}(e)}{6} = \frac{1}{6} \\
\Pr(\rho_{\text{sgn}}) &= 1 \cdot \frac{\chi_{\text{sgn}}(e)}{6} = \frac{1}{6} \\
\Pr(\rho_{\text{std}}) &= 2 \cdot \frac{\chi_{\text{std}}(e)}{6} = \frac{4}{6}
\end{align*}
\]

For the group $H = \langle (12) \rangle = \{e, (12)\} \cong \mathbb{Z}/2$:

\[
\begin{align*}
\Pr(\rho_{\text{triv}}) &= 1 \cdot \frac{\chi_{\text{triv}}(e)+\chi_{\text{triv}}((12))}{6} = \frac{(1+1)/6}{6} = \frac{2}{6} \\
\Pr(\rho_{\text{sgn}}) &= 1 \cdot \frac{\chi_{\text{sgn}}(e)+\chi_{\text{sgn}}((12))}{6} = \frac{(1-1)/6}{6} = 0 \\
\Pr(\rho_{\text{std}}) &= 2 \cdot \frac{\chi_{\text{std}}(e)+\chi_{\rho}((12))}{6} = 2 \cdot \frac{(2+0)/6}{6} = \frac{4}{6}
\end{align*}
\]
Sampling subgroups of $S_3$, continued

For the trivial group $\{e\}$:

\[
\begin{align*}
\Pr(\rho_{\text{triv}}) &= 1 \cdot \frac{\chi_{\text{triv}}(e)}{6} = 1/6 \\
\Pr(\rho_{\text{sgn}}) &= 1 \cdot \frac{\chi_{\text{sgn}}(e)}{6} = 1/6 \\
\Pr(\rho_{\text{std}}) &= 2 \cdot \frac{\chi_{\text{std}}(e)}{6} = 4/6
\end{align*}
\]

For the group $H = \langle (12) \rangle = \{e, (12)\} \cong \mathbb{Z}/2$:

\[
\begin{align*}
\Pr(\rho_{\text{triv}}) &= 1 \cdot \frac{\chi_{\text{triv}}(e) + \chi_{\text{triv}}((12))}{6} = (1 + 1)/6 = 2/6 \\
\Pr(\rho_{\text{sgn}}) &= 1 \cdot \frac{\chi_{\text{sgn}}(e) + \chi_{\text{sgn}}((12))}{6} = (1 - 1)/6 = 0 \\
\Pr(\rho_{\text{std}}) &= 2 \cdot \frac{\chi_{\text{std}}(e) + \chi_{\rho}(12)}{6} = 2 \cdot (2 + 0)/6 = 4/6
\end{align*}
\]

To distinguish $\langle (12) \rangle$ from the trivial group, we need to know with high probability that $\rho_{\text{sgn}}$ does not show up.
Negative results for $S_n$

Theorem (Hallgren-Russell-Ta-Shma, ’00) Fourier sampling cannot distinguish the trivial subgroup of $S_n$ from certain subgroups of order two in polynomial time with high probability.
Negative results for $S_n$

Theorem (Hallgren-Russell-Ta-Shma, ’00) Fourier sampling cannot distinguish the trivial subgroup of $S_n$ from certain subgroups of order two in polynomial time with high probability.

In particular, if $\Gamma_1$ and $\Gamma_2$ are two rigid graphs, then the isomorphism problem reduces to this case of the hidden subgroup problem.
Negative results for $S_n$

Theorem (Hallgren-Russell-Ta-Shma, ’00) Fourier sampling cannot distinguish the trivial subgroup of $S_n$ from certain subgroups of order two in polynomial time with high probability.

In particular, if $\Gamma_1$ and $\Gamma_2$ are two rigid graphs, then the isomorphism problem reduces to this case of the hidden subgroup problem.

Strong Fourier sampling is a variant of the algorithm where we keep track of not just the character of a representation $\rho$, but the whole matrix.
Negative results for $S_n$

**Theorem (Hallgren-Russell-Ta-Shma, ’00)** Fourier sampling cannot distinguish the trivial subgroup of $S_n$ from certain subgroups of order two in polynomial time with high probability.

In particular, if $\Gamma_1$ and $\Gamma_2$ are two rigid graphs, then the isomorphism problem reduces to this case of the hidden subgroup problem.

**Strong Fourier sampling** is a variant of the algorithm where we keep track of not just the character of a representation $\rho$, but the whole matrix.

**Theorem (Moore-Russell-Schulman, ’08)** Strong Fourier sampling also cannot distinguish hidden subgroups of $S_n$ in polynomial time with high probability.

**Question:** Can more intricate quantum algorithms efficiently solve the hidden subgroup problem for $S_n$?
References